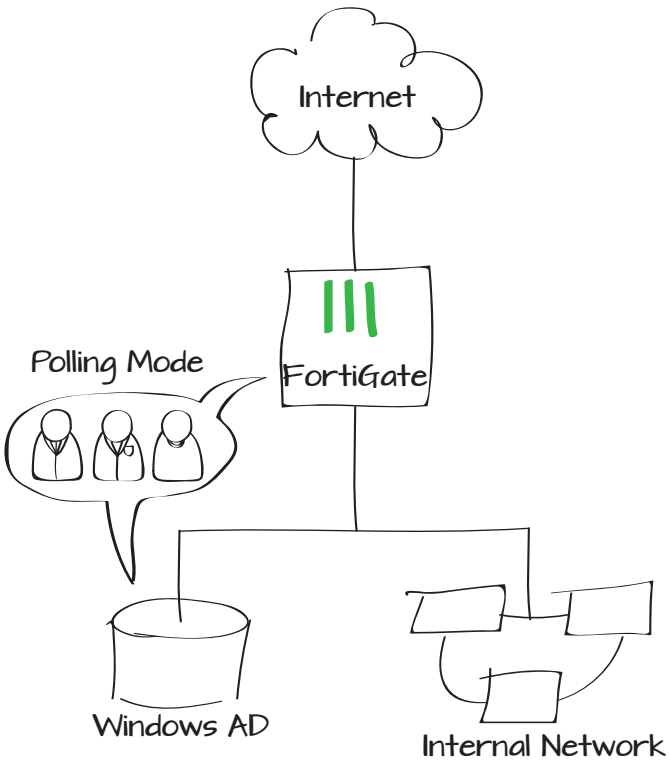
Fortinet Single Sign-On in Polling Mode for a Windows AD network

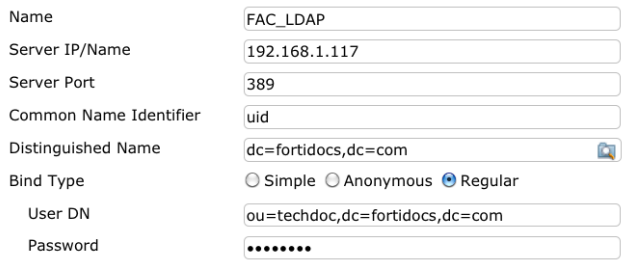
This example uses Active Directory Polling to establish Fortinet Single Sign-On (FSSO) for a Windows AD Domain Controller, without requiring a FortiAuthenticator or a Collector Agent running on the Windows AD Domain to act as an intermediary between the FortiGate and the domain.

1. Adding the LDAP Server to the FortiGate
2. Configuring the FortiGate unit to poll the Active Directory
3. Adding an FSSO user group
4. Adding a firewall address for the internal network
5. Adding a security policy that includes an authentication rule
6. Results



Adding the LDAP Server to the FortiGate

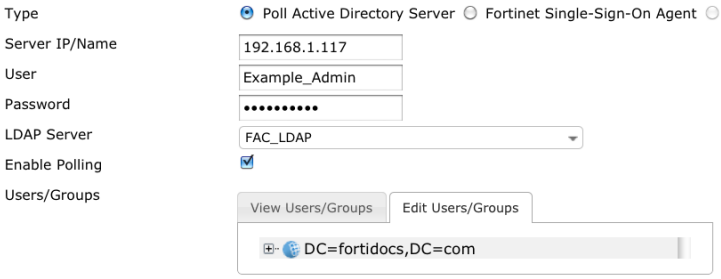
In the FortiGate web interface, go to **User & Device > Authentication > LDAP Servers**. Add your LDAP server details.



Configuring the FortiGate unit to poll the Active Directory

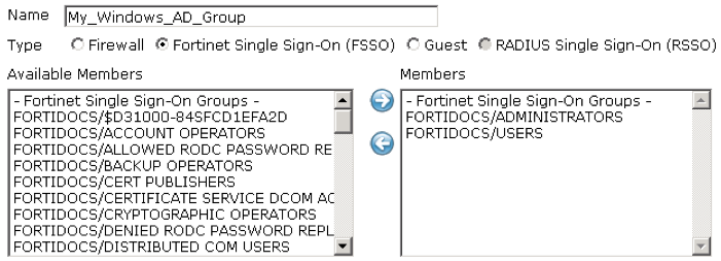
Next, go to **User & Device > Authentication > Single Sign-On**.

For the **Type**, select **Poll Active Directory Server**. Enter the IP, username and password, and select the LDAP server you added previously. Ensure **Enable Polling** is checked.



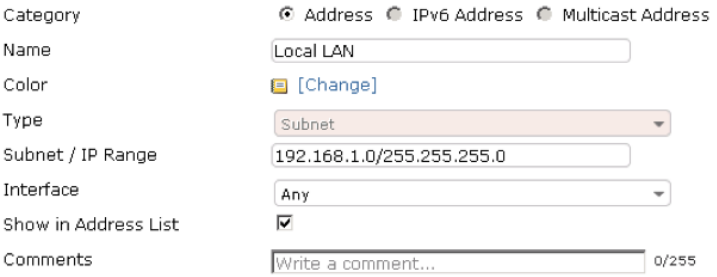
Adding an FSSO user group

Go to **User & Device > User > User Groups**, and add the desired AD member groups to the group.



Adding a firewall address for the internal network

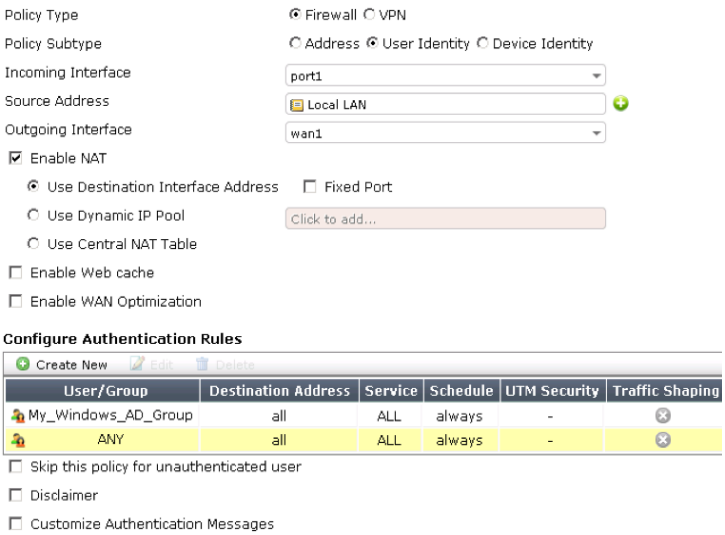
Go to **Firewall Objects > Address > Addresses**, and create an internal network address to be used by the policy.



Adding a security policy that includes an authentication rule

Go to **Policy > Policy > Policy**.

Create a **User Identity** policy and add an authentication rule to allow your FSSO group to access the internet.



Results

Go to **Log & Report > Traffic Log > Forward Traffic**. When users log into the Windows AD network, the FortiGate will automatically poll the domain for their account information, and record their traffic.

Select an entry for more information.

ate/Time	Src	Device	D
:49	ADMINISTRATOR (192.168.1.114)	00:0c:29:4b:d7:cc	204.246.169.91 (conte
:45	ADMINISTRATOR (192.168.1.114)	00:0c:29:4b:d7:cc	74.121.50.17 (www.pa
:07	TWHITE (192.168.1.116)	Lab test system 2	207.46.206.78 (mscrl.
:07	TWHITE (192.168.1.116)	Lab test system 2	207.46.206.78 (mscrl.
:04	TWHITE (192.168.1.116)	Lab test system 2	63.251.85.33 (m.webt
:04	TWHITE (192.168.1.116)	Lab test system 2	63.251.85.33 (m.webt
:04	TWHITE (192.168.1.116)	Lab test system 2	63.251.85.33 (m.webt

Dst	204.246.169.91 (content.mkt931.com)	**Virtual Domain**	root
Received	92	**Source Country**	Reserved
Src NAT IP	172.20.120.123	**Sent / Received**	292 B / 92 B
Device Type	Windows PC	**Duration**	10
Sent	292	**Src NAT Port**	9803
Application Details		**Group**	My_Windows_AD_Group
Device	00:0c:29:4b:d7:cc	**Service**	HTTP
Protocol	6	**byod_name**	
User	ADMINISTRATOR	**Destination Country**	United States
Identity Index	1	**Dst Port**	80
roll	65372	**Status**	close
Timestamp	Tue May 7 15:59:49 2013	**Tran Display**	snat
OS Name	Windows	**Sequence Number**	1607872
Policy ID	9	**Src Interface**	port1
Src	ADMINISTRATOR (192.168.1.114)	**Sent Packets**	7
OS Version	Vista	**Level**	notice
Src Port	9803	**Log ID**	13
Sub Type	forward	**Threat**	
Received Packets	2	**Date/Time**	15:59:49 (Tue May 7 15:59:49 2013)
Dst Interface	wan1		

Dst	207.46.206.78 (mscrl.microsoft.com)	**Virtual Domain**	root
Received	3202	**Source Country**	Reserved
Src NAT IP	172.20.120.123	**Sent / Received**	609 B / 3.13 KB
Device Type	Windows PC	**Duration**	5
Sent	609	**Src NAT Port**	50608
Application Details		**Group**	My_Windows_AD_Group
Device	Lab test system 2	**Service**	HTTP
Protocol	6	**byod_name**	Lab test system 2
User	TWHITE	**Destination Country**	United States
Identity Index	1	**Dst Port**	80
roll	65372	**Status**	close
Timestamp	Tue May 7 15:59:07 2013	**Tran Display**	snat
OS Name	Windows	**Sequence Number**	1607691
Policy ID	9	**Src Interface**	port1
Src	TWHITE (192.168.1.116)	**Sent Packets**	7
OS Version	7	**Level**	notice
Src Port	50608	**Log ID**	13
Sub Type	forward	**Threat**	
Received Packets	7	**Date/Time**	15:59:07 (Tue May 7 15:59:07 2013)
Dst Interface	wan1		